

DAFTAR ISI

KATA PENGANTAR	i
UCAPAN TERIMA KASIH	ii
ABSTRAK	iv
ABSTRACT	v
DAFTAR ISI	vi
DAFTAR GAMBAR	ix
DAFTAR TABEL	xi
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	5
1.3. Tujuan Penelitian	6
1.4. Batasan Masalah	6
1.5. Sistematika Penulisan	6
BAB II TINJAUAN PUSTAKA	8
2.1. Keamanan Informasi	8
2.2. Otentikasi	9
2.3. Kriptografi	10
2.3.1. Tujuan Kriptografi	11
2.3.2. Teknik Dasar Kriptografi	12
2.3.3. Karakteristik Kriptografi	13
2.3.4. Prinsip Shannon	14
2.4. <i>One Time Password</i> (OTP)	14
2.5. <i>Pseudo Random Number Generator</i> (PRNG)	16
2.6. <i>Data Encryption Standard</i> (DES)	18
2.6.1. Sejarah DES	18
2.6.2. Algoritma DES	18
2.7. Fungsi <i>Hash</i>	28
2.8. <i>Avalanche Effect</i>	29
2.9. <i>Randomness test</i>	29
2.10. Levenshtein	32
2.11. <i>SMS Gateway</i>	34

BAB III METODELOGI PENELITIAN	35
3.1. Desain Penelitian	35
3.2. Fokus Penelitian	38
3.3. Alat dan Bahan Penelitian	38
3.3.1. Alat Penelitian	38
3.3.2. Bahan Penelitian.....	39
3.4. Metode Penelitian	39
3.4.1. Metode Pengumpulan Data	39
3.4.2. Metode Pengembangan Perangkat Lunak	40
BAB IV HASIL PENELITIAN DAN PEMBAHASAN	42
4.1. Hasil Penelitian	42
4.2. Modifikasi Algoritma DES	43
4.2.1. Modifikasi PC-1	43
4.2.2. Modifikasi S-box	47
4.3. Pembangkitan dan Proses Pengiriman Kode Otentikasi	48
4.3.1. Alur Pembangkitan dan Pemecahan Kode Otentikasi	50
4.3.2. Proses Pengiriman Kode Otentikasi	52
4.4. Pengembangan perangkat lunak	53
4.4.1. Dekripsi Sistem	53
4.4.2. Batasan Perangkat Lunak	53
4.4.3. Proses Operasional Perangkat Lunak	54
4.4.4. Perancangan	54
4.4.5. Implementasi	55
4.4.6. Pengujian	63
4.5. Pembahasan Modifikasi Algoritma DES	63
4.5.1. Perbandingan Hasil Enkripsi	63
4.5.2. Pengujian Avalanche Effect	64
4.5.3. Pengujian Randomness Test	72
4.5.4. Percobaan <i>Exhaustive Attack</i>	79
4.5.5. Analisis Hasil Uji Modifikasi DES	80
BAB V KESIMPULAN DAN SARAN	84

5.1. Kesimpulan.....	84
5.2. Saran.....	85
DAFTAR PUSTAKA	86

DAFTAR GAMBAR

Gambar 2.1. CIA Triad (Stalling, 2011)	9
Gambar 2.2. Enkripsi dan dekripsi	11
Gambar 2.3. Flowchart Pembangkitan OTP mode <i>Self Generated</i>	16
Gambar 2.4. Struktur Global Algoritma DES (Munir, 2012)	19
Gambar 2.5. Jaringan fiestel pada satu putaran DES	20
Gambar 2.6. Skema Algoritma Enkripsi DES	20
Gambar 2.7. Proses pembangkitan kunci internal (Munir, 2012)	24
Gambar 2.8. Rincian komputasi fungsi f (Munir, 2012)	25
Gambar 2.9. Contoh Fungsi Hash	29
Gambar 2.10. Flowchart algoritma Levenshtein Distance (Rahayu, Pramono, & Dewi, 2015)	33
Gambar 3.1. Desain Penelitian	36
Gambar 3.2. Metode <i>Waterfall</i> (Sommerville, 2011)	40
Gambar 4.1. Kode Otentikasi Sosial Media melalui SMS	42
Gambar 4.2. Flowchart Perhitungan Nilai XOR Kunci	44
Gambar 4.3. Perubahan tabel PC-1 setelah di xor kunci	45
Gambar 4.4. Psudocode PC-1	45
Gambar 4.5. Modifikasi Right Row Left Row	46
Gambar 4.6. Perubahan tabel S-box setelah xor kunci	48
Gambar 4.7. Psudocode S-box	48
Gambar 4.8. Pembangkitan Kode Otentikasi	50
Gambar 4.9. Pemecahan Kode Otentikasi	51
Gambar 4.10. Proses Pengiriman Kode Otentikasi	52
Gambar 4.11. Use case sistem registrasi dan login	55
Gambar 4.12. Rancangan Basis data	55
Gambar 4.13. Tampilan aplikasi Main Menu	58
Gambar 4.14. Tampilan aplikasi DES standar	58
Gambar 4.15. Tampilan aplikasi DES modifikasi PC-1	59
Gambar 4.16. Tampilan aplikasi DES modifikasi S-box	59

Gambar 4.17. Tampilan DES modifikasi PC-1 dan S-box.....	60
Gambar 4.18. Tampilan <i>form</i> registrasi	61
Gambar 4.19. Kode otentikasi yang dikirim melalui SMS.....	61
Gambar 4.20. Tampilan form Aktivasi Akun.....	62
Gambar 4.21. Tampilan <i>form</i> login	62
Gambar 4.22. Tampilan Cryptool 1.4.30.....	72
Gambar 4.23. Memilih pengujian randomness test	73
Gambar 4.24. Tampilan eksekusi contoh randomness test.....	73
Gambar 4.25. Perubahan Hasil Avalanche Effect.....	82

DAFTAR TABEL

Tabel 2.1. Matriks permutasi Awal (IP)	21
Tabel 2.2. Matriks permutasi kompresi PC-1.....	22
Tabel 2.3. Posisi 28 bit K C ₀	22
Tabel 2.4. Posisi 28 bit K D ₀	22
Tabel 2.5. Pergeseran (Left Shift).....	23
Tabel 2.6. Matriks permutasi kompresi PC-2.....	23
Tabel 2.7. Posisi bit C _i	24
Tabel 2.8. Posisi bit D _i	24
Tabel 2.9. Matriks permutasi ekspansi	26
Tabel 2.10. S-box 1 dengan nilai awal 14	26
Tabel 2.11. S-box 2 dengan nilai awal 15	26
Tabel 2.12. S-box 3 dengan nilai awal 10	26
Tabel 2.13. S-box 4 dengan nilai awal 7.....	27
Tabel 2.14. S-box 5 dengan nilai awal 2.....	27
Tabel 2.15. S-box 6 dengan nilai awal 12	27
Tabel 2.16. S-box 7 dengan nilai awal 4.....	27
Tabel 2.17. S-box 8 dengan nilai awal 13	27
Tabel 2.18. Matriks permutasi P (P-box).....	27
Tabel 2.19. Matriks permutasi balikan (IP-1)	28
Tabel 2.20. R (Nilai Kritis) $\alpha = 0,05$ (Sonjaya, 2007).....	32
Tabel 2.21. Matriks Perhitungan Levenshtein <i>Distance</i>	34
Tabel 4.1. Model.....	56
Tabel 4.2. Controller.....	56
Tabel 4.3. View	57
Tabel 4.4. Library	57
Tabel 4.5. Pengujian Blackbox Sistem Registrasi	63
Tabel 4.6. Plainteks dan Kunci Perbandingan Hasil Enkripsi.....	63
Tabel 4.7. Perbandingan Hasil Enkripsi.....	64
Tabel 4.8. Kombinasi Kunci untuk Uji <i>Avalanche Effect</i>	64

Tabel 4.9. Uji Avalanche Effect kunci “37052676”	65
Tabel 4.10. Uji Avalanche Effect kunci “19220714”	66
Tabel 4.11. Uji Avalanche Effect kunci “43572392”	67
Tabel 4.12. Uji Avalanche Effect kunci “74035744”	68
Tabel 4.13. Uji Avalanche Effect kunci “35022452”	69
Tabel 4.14. Uji Avalanche Effect kunci “07979476”	70
Tabel 4.15. Uji Avalanche Effect dengan kunci “GIK207DA”	71
Tabel 4.16. Pengujian randomness dengan kunci “37052676”	74
Tabel 4.17. Pengujian randomness dengan kunci “19220714”	75
Tabel 4.18. Pengujian randomness dengan kunci “43572392”	75
Tabel 4.19. Pengujian randomness dengan kunci “74035744”	76
Tabel 4.20. Pengujian randomness dengan kunci “35022452”	76
Tabel 4. 21. Pengujian randomness dengan kunci “07979476”	77
Tabel 4. 22. Pengujian randomness dengan kunci “GIK207DA”	78
Tabel 4.23. Uji <i>randomness test</i> terhadap hasil enkripsi pada sistem registrasi ...	78
Tabel 4.24. Analisis Levenshtein Pada Kode Otentikasi ca02fd	79
Tabel 4.25. Analisis Levenshtein Pada Kode Otentikasi 24a936	79
Tabel 4.26. Analisis Levenshtein Pada Kode Otentikasi 9f87f3	80
Tabel 4.27. Hasil uji modifikasi algoritma DES	81
Tabel 4.28. Hasil Uji Avalanche Effect	81

LAMPIRAN

Lampiran 1. Hasil *Avalanche effect* dengan percobaan 30 kunci pada plainteks “ilkom695”